Avadeen Consulting White Paper

Risk Management Framework for Superannuation Funds

Indicative RMF in compliance with SPS220

Tiger Pillay
Feb 2025

1. Background

CPS220 vs SPS220

Super funds do not need to comply with both standards separately. Instead, they comply with SPS 220, which was drafted to be consistent with CPS 220 but tailored to the superannuation context.

That means SPS 220 covers the core elements of risk management (framework, strategy, board accountability) while adding super-specific obligations such as:

- Outsourcing of administration
- Insurance in superannuation
- Conflicts management

In practice:

- CPS 220 = cross-industry baseline (banks, insurers, supers).
- SPS 220 = superannuation-specific version that replaces CPS 220 for RSE licensees.

Both reinforce the same principle: Boards remain ultimately accountable for effective risk management.

Overlapping prudential standards

APRA and ASIC's prudential and conduct standards form an interconnected framework of governance, risk and accountability.

SPS 220 (Risk Management): establishes the risk management framework for super funds.

SPS 515 (Strategic Planning & Member Outcomes): links risk to strategy, requiring funds to prove they deliver value to members.

CPS 230 (Operational Risk Management): effective July 2025, lifts expectations on operational resilience, service providers and continuity of critical operations.

CPS 234 (Information Security): ensures entities safeguard information assets and maintain cyber resilience.

FAR (Financial Accountability Regime): extends personal accountability to directors and senior executives for risk management, compliance and resilience.

Together they create a unified expectation:
Boards and executives must align risk, strategy, resilience and accountability into a single operating model.

- SPS 220 + SPS 515 = governance and strategic baseline.
- CPS 230 + CPS 234 = operational and cyber resilience depth.
- FAR = personal accountability overlay.

The result: stronger protection of members, customers and the financial system

2. Oversight of Risk Management Framework

Risk governance structure

SPS 220 (Risk Management) places ultimate accountability squarely with the Board of an RSE licensee.

Board Responsibilities:

- Approve and maintain the Risk Management Framework (RMF) and Risk Management Strategy (RMS).
- Provide an annual Risk Management Declaration to APRA confirming the RMF is effective and compliant.

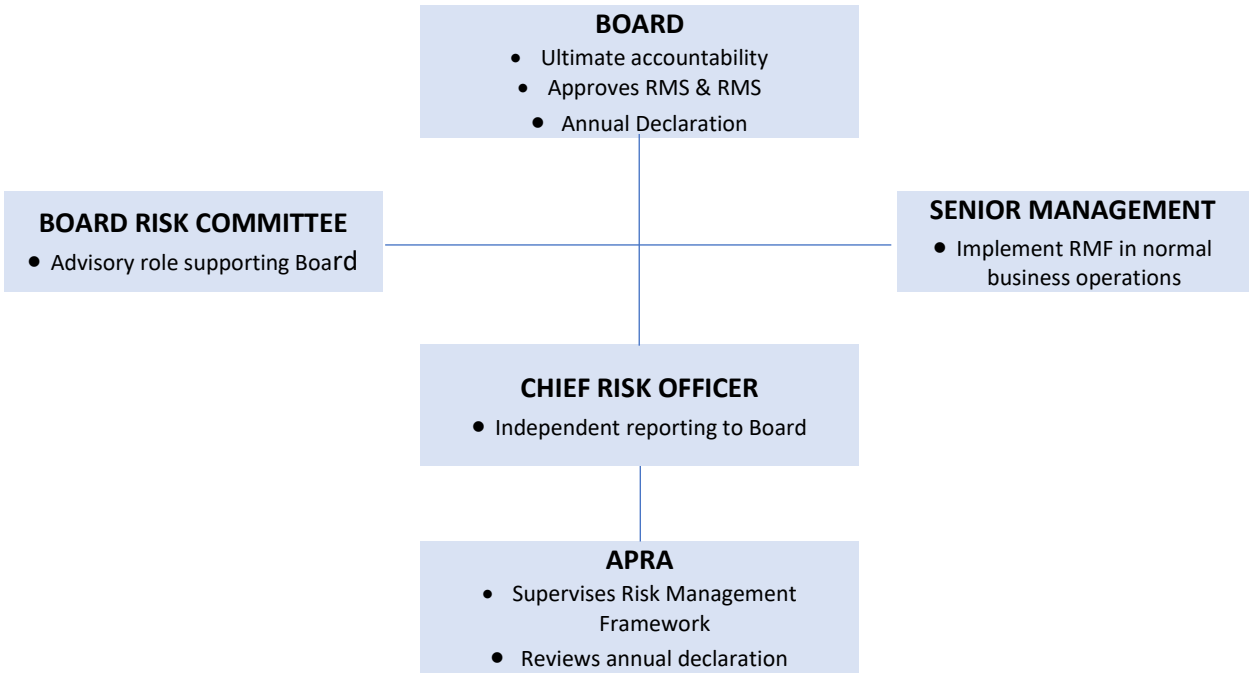
Senior Management & Risk Functions:

- Implement the RMF in day-to-day operations.
- Support the Board via a Risk Committee or equivalent.
- Ensure the CRO (Chief Risk Officer) has independence to challenge decisions and report directly to the Board.

APRA Oversight:

- Reviews RMF effectiveness and Board governance.
- Links failures to broader accountability frameworks, including FAR.

Boards cannot delegate responsibility — oversight of SPS 220 is a Board-level obligation, backed by senior management, risk functions, and APRA supervision.



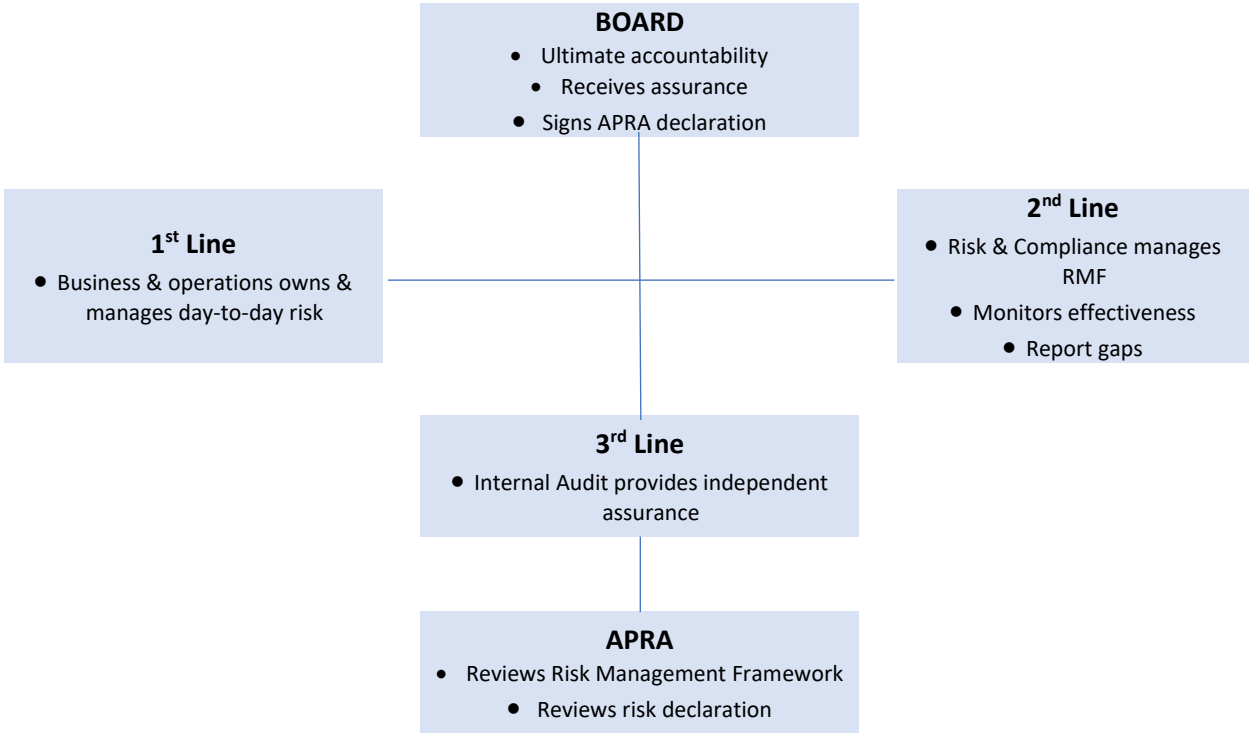
Assurance & review

Assurance and review of SPS 220 and the RMF rely on a three-tiered approach: operational ownership (first line), independent oversight (second line), and independent verification (third line), all overseen by the Board and monitored by APRA.

- 1st Line – Operational Ownership: Business teams manage risks day-to-day and ensure controls are effective.
- 2nd Line – Independent Oversight: Risk and compliance functions monitor the RMF, challenge the 1st line, and report to the Board.
- 3rd Line – Independent Verification: Internal audit provides assurance that risk management and controls are effective.

All three lines are overseen by the Board, which holds ultimate accountability, and monitored by APRA to ensure compliance with SPS 220.

A structured, layered assurance model ensures risk is managed effectively, governance is robust, and member outcomes are protected.



Integration with member outcomes

In superannuation funds, risk management and member outcomes must be fully aligned:

- RMF (SPS 220) – Identifies and manages all material risks: operational, investment, compliance, outsourcing, insurance.
- Member Outcomes (SPS 515) – Includes investment returns, fees, insurance, and service quality.

Integration in Practice:

- Risk-aware strategy: All initiatives are evaluated against the RMF to ensure risks remain within appetite and protect members.
- Embedded controls: Operational and compliance risks are managed to prevent negative impacts on member outcomes.
- Board oversight & assurance: Ensures risk reporting and strategic decisions consistently safeguard member interests.
- Continuous monitoring: KPIs track both risk exposure and delivery of member outcomes, enabling ongoing improvement.

A fund that is strategically focused, risk-aware, and member-centric, with governance, risk, and assurance aligned to protect members and deliver value.

3. Core components of a Risk Management Framework

A SPS 220-compliant RMF that incorporates SPS515, CPS 230, CPS 234, and FAR will have:

1. Governance & Accountability
    - Three Lines of Defence.
    - FAR accountability mapping.
2. Risk Taxonomy (expanded)
    - Strategic, investment, operational, compliance, conduct, reputational.
    - Operational Resilience (CPS 230).
    - Cyber / Information Security (CPS 234).
3. Risk Appetite & Strategy
    - Appetite for operational disruptions and cyber events explicitly defined.
    - Link to continuity, outsourcing, and incident response.
4. Processes
    - Incident & breach management aligned with CPS 230 & CPS 234 reporting.
    - Testing regime (BCP, cyber resilience, service provider continuity).
5. Assurance
    - Internal audit testing includes operational resilience and cyber.
    - Independent RMF review covers new standards.

.

Recommended specific inclusions

- Risk governance defines accountability of Board, Risk Committee and Senior Management
- Risk Appetite Statement (& tolerance) defines level and type of risk the fund is willing to accept
- Risk Management Strategy Documents how material risks will be identified, assessed, monitored, managed, and reported.
- Risk Register defines requirement to capture, monitor, and manage all material risks (including investment, operational, outsourcing, cyber, regulatory, strategic, conduct, reputational).
- Risk Taxonomy that is a structured classification system for risks. It defines categories and subcategories so that all risks across the fund are consistently identified, assessed, and reported
- Business plan alignment – need to ensure that RMF is integrated with the fund's strategic and business planning processes.
- Aligned policies & procedures defines integrated risk and compliance policies and how they contribute to a robust risk management environment.
- Core risk management processes that include identification, assessment, controls, monitoring and reporting of risks
- Risk culture framework that defines training, awareness, and behaviours that support good risk outcomes
- Three lines of defence (LOD) matrix defines specific roles and responsibilities to ensure robust risk management, accountability and assurance.

Appendix: SPS220 Compliant Risk Management Framework (RMF) template (incorporates the new obligations from CPS 230, CPS 234, and FAR)

1. Introduction

- Purpose and objectives of the RMF.
- Alignment with:
  - SPS 220 (Risk Management – superannuation).
  - CPS 230 (Operational Risk Management & Resilience).
  - CPS 234 (Information Security).
  - FAR (Financial Accountability Regime).
- Scope (all activities, subsidiaries, outsourced providers).

2. Governance & Accountability

- Board Responsibilities
  - Ultimate accountability for risk management and member outcomes.
  - Approves Risk Appetite Statement (RAS), Risk Management Strategy (RMS), and RMF.
- Board Committees
  - Audit & Risk Committee / Investment Committee oversight.
  - Monitoring of operational resilience and cyber posture.
- Executive Management
  - Responsible for implementing RMF across first line.
- Three Lines of Defence model
  - Business units (1st line), risk/compliance (2nd line), internal audit (3rd line).
- FAR Mapping
  - Clear accountability of "Accountable Persons" (Board, CEO, CRO, CIO, COO, CISO, etc.).
  - RACI chart linking risk classes to accountable persons.

3. Risk Appetite Statement (RAS)

- Defines risk boundaries, including:
  - Strategic, investment, compliance, conduct, reputational.
  - Operational risk appetite (CPS 230).
  - Cyber/information security appetite (CPS 234).
- Tolerances & metrics:
  - Maximum downtime for critical operations.
  - Acceptable level of member service failures.
  - Cyber resilience metrics (e.g. penetration testing, phishing success rates).

4. Risk Management Strategy (RMS)

- Outlines how the RMF operates.
- Integration into:
  - Strategic & business planning.
  - Product design.
  - Service provider arrangements.
  - FAR accountability governance.
- Process for continuous improvement and APRA reporting.

5. Risk Taxonomy

- Strategic Risk
- Investment Risk
- Operational Risk (expanded per CPS 230):
    - Critical operations identification.
    - Outsourcing/service provider risk.
    - Business continuity and disruption events.
- Information Security / Cyber Risk (CPS 234)
- Compliance & Legal Risk
- Conduct & Reputational Risk

6. Risk Management Process

- Identification: risk assessments, incident and breach reporting (aligned to CPS 230/234).
- Assessment: risk scoring methodology, scenario analysis, stress testing.
- Controls: mapped to risks, including operational resilience and information security controls.
- Monitoring: KRIs/KPIs linked to operational resilience and cyber (uptime, recovery time, incidents, audit results).
- Reporting: structured risk reports to management, Board, and APRA.

7. Policies Supporting the RMF

- Risk Management Policy.
- Compliance Policy.
- Conflicts Management Policy.
- Outsourcing & Service Provider Policy (CPS 230, SPS 231).
- Operational Risk & Resilience Policy (CPS 230).
- Incident & Breach Management Policy (CPS 230/234).
- Information Security Policy (CPS 234).
- Business Continuity & Disaster Recovery Policy.

8. Risk Culture

- Risk culture expectations & trustee behaviours.
- Staff and trustee training programs (including cyber awareness).
- Escalation pathways for risk incidents.
- Monitoring through surveys, observations, whistleblower reports.

9. Assurance & Independent Review

- Internal audit program covering all major risk categories.
- **Independent triennial RMF review** (SPS 220 requirement).
- Assurance over:
    - Operational resilience testing (CPS 230).
    - Cyber control testing (CPS 234).
- Tracking and reporting of remediation actions to the Board.

10. Member Outcomes Integration (SPS 515)

- Show how RMF supports:
  - Net investment returns.
  - Service quality and complaint handling.
  - Member data protection.
  - Value-for-money outcomes.

11. Reporting Framework

- Risk dashboards for management, committees, and Board.
- FAR accountability reports showing who owns each risk outcome.
- Escalation triggers for APRA notifications (material breaches, cyber events, service disruptions).

12. Continuous Improvement

- RMF reviewed:
  - Annually.
  - After material incidents (e.g., cyber-attack, service disruption).
  - Following APRA or internal audit feedback.
- Process for updating RAS, RMS, and policies.

Appendices

- A. Risk Register Template (with CPS 230 & CPS 234 categories).
- B. KRI/KPI Dashboard Example (uptime, cyber incidents, complaints).
- C. FAR Accountability Matrix.
- D. Business Continuity Critical Operations Map.